UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/530,122	02/23/2010	Tatsuo Nomura	63227(72039)	2625

21874 7590 06/24/2010

EDWARDS ANGELL PALMER & DODGE LLP
P.O. BOX 55874
BOSTON, MA 02205

EXAMINER	
RAHMAN, MAHFUZUR	
ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
06/24/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/530,122	NOMURA ET AL.	
	Examiner	Art Unit	
	MAHFUZUR RAHMAN	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/23/2010, 4/1/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Applicant's amendment filed 04/01/2005 is acknowledged. Claims 1-2 have been amended. Claims 1-6 are examined and pending.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 2/23/2010 and 4/1/2005 have been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Oath/Declaration

The Oath/Declaration filed on 3/23/2010 is accepted by the examiner.

Drawings

The drawings filed on 4/1/2005 are accepted by the examiner.

Priority

The application is filed on 2/23/2010 and this is a 371 of PCT/JP2003/012561filed 10/01/2003. The application claims the benefit of foreign application number JAPAN 2002-288629 filed on 10/01/2002.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Verma et al. (US 2003/0115326 A1, hereinafter, Verma) in view of Olsen et al. (US 2002/0016921 A1, hereinafter, Olsen).

Regarding Claim 1, Verma discloses an image processing device, comprising:

a plurality of image data processing means which have different security levels and which process inputted image data (Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons; Fig. 1: plurality of image data processing means); and

a plurality of image data processing requesting means which request any of the image data processing means to process image data (Paragraph 0105: Job Manager 404 creates a job by passing a request to a Document Queue Manager (DQM) 408. The DQM 408 creates a job record, and returns a job-ID to the Job Manager), characterized in that:

the image data processing requesting means have a function [to verify security levels] of second image data processing means to which the image data processing is to be requested (Paragraph 0101: check the status of the appliance queue associated with the selected device; Paragraph 0114: the destination type is for printing the job (i.e., in response to a "print" function), the Distribution Print Agent 600 communicates with the Configuration Manager 500 to determine other details, such as queue name, and printer hostname/IP) and

then request the second image data processing means to perform -distributed processing of image data in addition to an image data processing means first requested to process the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202; Paragraph 0089: in response to a print command, additionally, the thin client 224 suitably communicates with a remote DMM 232 of a second appliance 234).

Verma does not explicitly discloses but Olsen from the same or similar fields of endeavor teaches verifying security levels in image processing system (Paragraph 0033: the user table includes system user name, system user ID, system user credit, system user's access rights, system user's server address, system user identifying number, system user PUK code (personal user key), system user initiation date or any combination thereof, and a second user pin code. The control unit transmits upon receipt of the first pin code the user identifying data to the server for verification; Paragraph 0067: The front-end module 124 subsequently verifies the user's identity by checking the pin code. If the pin code is not in accordance with the pin code registered in the server 136 for that particular user, then the display 126 informs the user that access is denied. If the pin code is in accordance with the pin code registered in the server 136 for that particular user, then the front-end module 124 requests print jobs from the control unit 120. However, only print jobs, which the particular verified user is

allowed to perform. The control unit 120 in turn requests this information from the server 136 checking the user table 114 in the job database 110. The verified user may then view a document list, select to printing of any of the print jobs or viewing any of the print jobs on the display 126, which print jobs are designated to the verified user).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to verify security levels (Paragraph 0415: Clients can only perform this command with a security level of Power User or Administrator) as taught by Olsen in the teachings of Verma for the advantage of ensuring secure transfer of documents from a client connected to a network such as a local area network (LAN) or a wide area network (WAN) to a user who is allowed access to the documents from a printing communication unit connected to a printer (Paragraph 0001).

Regarding Claim 2, the combination of Verma and Olsen discloses the image processing device according to claim 1, characterized in that the image data processing requesting means have a function to select, from among the plurality of image data processing means, all other image data processing means whose security level is equal to or higher than the security level of the image data processing means first requested to process the image data (Verma, Paragraph 0207: The appliance architecture recognizes the following user archetypes: Administrator, Power User, and User. The appliance 200 allows for the grouping of users into user groups. A Power User and Administrator can only create/delete a group and add/delete members to the group.

Grouping is only available for the DMM component, and is basically done to simplify the sharing of resources (Folders, etc.)), and

a function to request the selected second image data processing means to perform distributed processing of the image data (Verma, Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons; Paragraph 0093: if the user intends to send the job to multiple destinations, then the user selects the destination printer(s) and load a previously-stored job delivery profile).

Regarding Claim 3, Verma discloses an image processing device, comprising:

a plurality of image data processing means which have different security levels and which process inputted image data (Paragraph 0081: The system 100 includes a network-based document service appliance 102 (i.e. iSP appliance for image Service Platform appliance) that is a document distribution solution with document management capabilities and device management support; Fig. 1: plurality of image data processing means); and

an image data processing requesting means which request any of the image data processing means to process image data (Paragraph 0105: Job Manager 404 creates a job by passing a request to a Document Queue Manager (DQM) 408. The DQM 408 creates a job record, and returns a job-ID to the Job Manager), characterized in that:

the image data processing requesting means have a function [to verify a security level] of a second image data processing means to which the image data processing is to be requested (Paragraph 0114: the destination type is for printing the job (i.e., in response to a "print" function), the Distribution Print Agent 600 communicates with the Configuration Manager 500 to determine other details, such as queue name, and printer hostname/IP; Paragraph 0101: check the status of the appliance queue associated with the selected device) and

then request the second image data processing means to perform alternate processing of the image data (Paragraph 0201: a facility is provided to the user through which aged files (documents that were not accessed within a specified period of time) are automatically moved to an alternative location)

in place of an image data processing means first requested to process the image data if the first image data processing means can no longer continue processing subsequent part of the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202).

Verma does not explicitly discloses but Olsen from the same or similar fields of endeavor teaches verifying security levels in image processing system (Paragraph 0033: the user table includes system user name, system user ID, system user credit,

system user's access rights, system user's server address, system user identifying number, system user PUK code (personal user key), system user initiation date or any combination thereof, and a second user pin code. The control unit transmits upon receipt of the first pin code the user identifying data to the server for verification; Paragraph 0067: The front-end module 124 subsequently verifies the user's identity by checking the pin code. If the pin code is not in accordance with the pin code registered in the server 136 for that particular user, then the display 126 informs the user that access is denied. If the pin code is in accordance with the pin code registered in the server 136 for that particular user, then the front-end module 124 requests print jobs from the control unit 120. However, only print jobs, which the particular verified user is allowed to perform. The control unit 120 in turn requests this information from the server 136 checking the user table 114 in the job database 110. The verified user may then view a document list, select to printing of any of the print jobs or viewing any of the print jobs on the display 126, which print jobs are designated to the verified user).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to verify security levels (Paragraph 0415: Clients can only perform this command with a security level of Power User or Administrator) as taught by Olsen in the teachings of Verma for the advantage of providing means for a client station to designate a document to a single user or a group of users and providing the possibility for the single user or the group of users to access the document at a plurality of printer communication units (Paragraph 0001).

Regarding Claim 4, the combination of Verma and Olsen discloses the image processing device according to claim 3, characterized in that the image data processing requesting means have a function to select, from among the plurality of image data processing means, all other image data processing means whose security level is equal to or higher than the security level of the image data processing means first requested to process the image data (Verma, Paragraph 0207: The appliance architecture recognizes the following user archetypes: Administrator, Power User, and User. The appliance 200 allows for the grouping of users into user groups. A Power User and Administrator can only create/delete a group and add/delete members to the group. Grouping is only available for the DMM component, and is basically done to simplify the sharing of resources (Folders, etc.), and

a function to request the selected second image data processing means to perform alternate processing of subsequent part of the image data (Verma, Paragraph 0265: subsequent "Print File" operations; Paragraph 0093: if the user intends to send the job to multiple destinations, then the user selects the destination printer(s) and load a previously-stored job delivery profile).

Regarding Claim 5, Verma discloses an image processing system, comprising:

a plurality of image data processing means which have different security levels and which process inputted image data (Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600

wherein 0152: access to DMM objects is restricted to authorized users for security reasons; Fig. 1: plurality of image data processing means); and

an image data processing requesting means which request any of the image data processing means to process image data (Paragraph 0105: Job Manager 404 creates a job by passing a request to a Document Queue Manager (DQM) 408. The DQM 408 creates a job record, and returns a job-ID to the Job Manager), where

the image processing system distributes image data received from the image data processing requesting means to second image data processing means available for distributed processing in addition to an image data processing means first requested to process the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202), characterized in that:

the data processing requesting means have a function [to verify security levels] of the second image data processing means to which the image data distributed processing is to be requested (Paragraph 0101: check the status of the appliance queue associated with the selected device; Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons) and

then request the second image data processing means to perform distributed processing of the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202); and

the second image data processing means have a function to perform distributed processing of the image data in conjunction with the image data processing means first requested to process the image data (Paragraph 0089: Documents 228 input to the thick client 222 are opened within a native application 230, and sent to the thick client 222 in response to a print command of the native application 230. Since the thin client 224 is browser-based for selecting documents from a server, the documents 228 are uploaded to the thin client 228. Additionally, the thin client 224 suitably communicates with a remote DMM 232 of a second appliance 234).

Verma does not explicitly discloses but Olsen from the same or similar fields of endeavor teaches verifying security levels in image processing system (Paragraph 0033: the user table includes system user name, system user ID, system user credit, system user's access rights, system user's server address, system user identifying number, system user PUK code (personal user key), system user initiation date or any combination thereof, and a second user pin code. The control unit transmits upon

receipt of the first pin code the user identifying data to the server for verification; Paragraph 0067: The front-end module 124 subsequently verifies the user's identity by checking the pin code. If the pin code is not in accordance with the pin code registered in the server 136 for that particular user, then the display 126 informs the user that access is denied. If the pin code is in accordance with the pin code registered in the server 136 for that particular user, then the front-end module 124 requests print jobs from the control unit 120. However, only print jobs, which the particular verified user is allowed to perform. The control unit 120 in turn requests this information from the server 136 checking the user table 114 in the job database 110. The verified user may then view a document list, select to printing of any of the print jobs or viewing any of the print jobs on the display 126, which print jobs are designated to the verified user).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to verify security levels (Paragraph 0415: Clients can only perform this command with a security level of Power User or Administrator)as taught by Olsen in the teachings of Verma for the advantage of ensuring secure transfer of documents from a client connected to a network such as a local area network (LAN) or a wide area network (WAN) to a user who is allowed access to the documents from a printing communication unit connected to a printer (Paragraph 0001).

Regarding Claim 6, Verma discloses an image processing system, comprising:

a plurality of image data processing means which have different security levels and which process inputted image data (Paragraph 0169: Depending on the provided

access rights, the user can perform a wide variety of operations on documents 1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons; Fig. 1: plurality of image data processing means); and

image data processing requesting means which request any of the image data processing means to process image data (Paragraph 0105: Job Manager 404 creates a job by passing a request to a Document Queue Manager (DQM) 408. The DQM 408 creates a job record, and returns a job-ID to the Job Manager), where

the image processing system alternated processes image data inputted by the image data processing requesting means to a second image data processing means available for alternate processing in place of an image data processing means first requested to process the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202), characterized in that:

the image data processing requesting means have a function [to verify a security level] of the second image data processing means to which the image data alternate processing is to be requested (Paragraph 0101: check the status of the appliance queue associated with the selected device; Paragraph 0169: Depending on the provided access rights, the user can perform a wide variety of operations on documents

1600 wherein 0152: access to DMM objects is restricted to authorized users for security reasons) and

then request the second image data processing means to perform alternate processing of the inputted image data if the first image. data processing means first requested to process the image data can no longer continue processing subsequent part of the image data (Paragraph 0199: the user is granted access in accordance to rights assigned by the Administrator. Flow is then to a decision block 1912 to determine if the user chooses to move or copy a file from one location to another. If not, flow is out the "N" path to the input of the decision block 1912. If so, flow is out the "Y" path to a decision block 1914 to determine if the file action is within the DMM 202); and

the second image data processing means has a function to perform alternate processing of the subsequent part of the image data in place of the image data processing means first requested to process the image data (Paragraph 0202: Additionally, a facility is provided to the user through which aged files (documents that were not accessed within a specified period of time) are automatically moved to an alternative location).

Verma does not explicitly discloses but Olsen from the same or similar fields of endeavor teaches verifying security levels in image processing system (Paragraph 0033: the user table includes system user name, system user ID, system user credit, system user's access rights, system user's server address, system user identifying number, system user PUK code (personal user key), system user initiation date or any combination thereof, and a second user pin code. The control unit transmits upon

receipt of the first pin code the user identifying data to the server for verification; Paragraph 0067: The front-end module 124 subsequently verifies the user's identity by checking the pin code. If the pin code is not in accordance with the pin code registered in the server 136 for that particular user, then the display 126 informs the user that access is denied. If the pin code is in accordance with the pin code registered in the server 136 for that particular user, then the front-end module 124 requests print jobs from the control unit 120. However, only print jobs, which the particular verified user is allowed to perform. The control unit 120 in turn requests this information from the server 136 checking the user table 114 in the job database 110. The verified user may then view a document list, select to printing of any of the print jobs or viewing any of the print jobs on the display 126, which print jobs are designated to the verified user).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to verify security levels (Paragraph 0415: Clients can only perform this command with a security level of Power User or Administrator)as taught by Olsen in the teachings of Verma for the advantage of providing means for a client station to designate a document to a single user or a group of users and providing the possibility for the single user or the group of users to access the document at a plurality of printer communication units (Paragraph 0001).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Sakai et al. Patent No. 5,703,696 discloses Image memory apparatus.
- Lupien, Jr. et al. Patent No. US 6,738,158 B1 discloses Digital scanner for capturing and processing images.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571) - 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R./

Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438